NAT'L INST OF STAND & TECH R.I.C.
A11103 981425
NIST
PUBLICATIONS

NISTIR 5153

Minimum Security Requirements for Multi-User Operating Systems

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

QC
100
.U56
#5153
1993

NIST

NISTIR 5153

Minimum Security Requirements for Multi-User Operating Systems

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

March 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Raymond G. Kammer, Acting Director

A Protection Profile for the
U.S. Information Security Standard

NOTE: THIS DOCUMENT HAS BEEN SUPERSEDED BY THE FEDERAL CRITERIA.

Abstract

The Minimum Security Requirements for Multi-User Operating Systems (MSR) document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems. The MSR document was written from the prospective of protecting the confidentiality and integrity of an organization's resources and promoting the continual availability of these resources. The MSR presented in this document form the basis for the commercially oriented protection profiles in Volume II of the draft *Federal Criteria for Information Technology Security* document (known as the Federal Criteria). The Federal Criteria is currently a draft and supersedes this document.

The MSR document has been developed by the MSR Working Group of the Federal Criteria Project under National Institute of Standards and Technology (NIST) leadership with a high level of private sector participation. Its contents are based on the Trusted Computer System Evaluation Criteria (TCSEC) C2 criteria class, with additions from current computer industry practice and commercial security requirements specifications.

TABLE OF CONTENTS

SECTION PAGE

Abstract ii

1. Introduction 1-1

1.1 Background 1-1
1.1.1 Trusted Computer System Evaluation Criteria (TCSEC) 1-2
1.1.2 Information Technology Security Evaluation Criteria (ITSEC) 1-2
1.1.3 Security Requirements in the Commercial Sector 1-3
1.1.4 System Security Study Committee 1-4
1.1.5 Federal Criteria Project 1-5
1.1.6 Minimum Security Requirements 1-5
1.2 Scope of the MSR 1-6
1.3 Audience 1-6
1.4 Terminology 1-7
1.5 Document Organization 1-7

2. Rationale 2-1

2.1 Intended Method of Use 2-1
2.2 Environmental Assumptions 2-1
2.3 Expected Threats 2-2
2.4 Security Features and Assurances 2-2
2.4.1 Identification and Authentication 2-3
2.4.2 Access Control 2-3
2.4.3 Audit 2-3
2.4.4 System Integrity 2-4
2.4.5 Data Integrity 2-4
2.4.6 Reliability of Service 2-4
2.4.7 Product Development Assurance 2-4
2.4.8 Product Documentation Assurance 2-5

SECTION PAGE

3. Functionality Requirements 3-1

3.1 Identification and Authentication 3-1
3.1.1 Identification 3-1
3.1.2 Authentication 3-3
3.1.2.1 Password Requirements 3-4
3.2 Access Control 3-7
3.2.1 System Access Control 3-7
3.2.2 Resource Access Control 3-10
3.2.2.1 Object Reuse 3-12
3.2.3 Privileges 3-12
3.3 Audit 3-13
3.3.1 Data Recording 3-13
3.3.2 Data Reporting 3-16
3.4 System Integrity 3-17
3.5 Data Integrity 3-18
3.6 Reliability of Service 3-18

4. Assurance Requirements 4-1

4.1 Product Development Assurances 4-1
4.2 Product Documentation Assurances 4-1
4.2.1 User Documentation 4-2
4.2.2 Administrator Documentation 4-2
4.2.3 Operator Documentation 4-3

Appendix: Threat Analysis APX-1

References REF-1

Glossary of Acronyms and Terms GL-1

1. INTRODUCTION

Government and commercial organizations rely heavily on information technology (IT) products to meet their operational, financial, and information requirements. The confidentiality, integrity, and availability of key software systems, databases, and data networks are major concerns throughout these sectors. The corruption, unauthorized disclosure, or theft of an organization's electronically-maintained resources can have a disruptive effect on the continuity of operations as well as serious and immediate financial, legal, and public confidence impact.

The Minimum Security Requirements (MSR) contained in this document are intended to provide both government and commercial organizations with a basic set of security requirements to protect the confidentiality and integrity of an organization's resources and to promote the continual availability of these resources.

1.1 BACKGROUND

In 1991, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established a joint project, termed the *Federal Criteria for Information Technology Security* (known as the Federal Criteria Project), to develop new Federal Criteria for Trusted Systems Technology. The purpose of this project is to produce a Federal Information Processing Standard (FIPS) on developing, specifying, and evaluating IT security products that will:

- Be consistent with international marketplace demands
- Provide for mutual recognition of security evaluation results between the United States and the European Community
- Replace the existing Trusted Computer System Evaluation Criteria (TCSEC) [1] with a second generation iteration that has a less restrictive approach and wider commercial appeal
- Provide for the open distributed computing environment of the 1990's and beyond

The MSR form the basis of one of the protection profiles of volume II of the preliminary Federal Criteria FIPS, the CS2, as mentioned in section 1.1. It is hoped that this Protection Profile, if widely accepted, will form the basis for mutual recognition of system evaluations between nations.

The MSR specify a set of security requirements needed in a class of products colloquially called "general purpose, multi-user operating systems". These requirements have been developed by the MSR Working Group of the Federal Criteria Project under NIST leadership with a high level of private sector participation. They are based on the TCSEC C2 criteria class, with additions from

current computer industry practice, from commercial security requirements specifications, and from the on-going work of the Federal Criteria Project.

The following sub-sections provide descriptions of each of these sources, and also further background on the motivation for and development of the MSR.

1.1.1 Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC [1], originally published in 1983 and revised in 1985, was the first publicly available document that expressed general security requirements that could apply to a specific class of technology (e.g., operating systems). It represents the culmination of many years of effort to address IT security issues within the Department of Defense (DoD) classified world. Since its publication, the TCSEC has influenced vendors, consumers, and the authors of other requirements documents both in the U.S. and abroad. The impact of the TCSEC on the field of IT security is widely recognized.

The TCSEC is made up of IT security features and assurances derived and engineered to support a very specific DoD security policy -- the prevention of unauthorized disclosure, or "leakage," of classified information (i.e., confidentiality). Although it has been helpful, the TCSEC does not completely address the security requirements of organizations handling sensitive (but unclassified) information. Besides confidentiality, organizations outside the classified world are also concerned with the other two components of security --integrity and availability.

Until recently, the government paid more attention to classified information processing than to addressing the IT security needs of commercial and government organizations that process unclassified sensitive information. During the past few years, commercial and government organizations processing sensitive information have begun to pay increasing attention to IT security needs. Although the TCSEC-motivated security features address some security problems, these features do not provide a complete solution. TCSEC requirements were specified because a more appropriate set of security functions was not been available.

The MSR is intended to be the first step in providing a set of security requirements appropriate for commercial and government organizations concerned with protecting sensitive information.

1.1.2 Information Technology Security Evaluation Criteria (ITSEC)

In recognition of the fact that a harmonized criteria was necessary to permit the mutual recognition of evaluation results, Germany, France, the United Kingdom, and the Netherlands created a harmonized set of security criteria referred to as the *Information Technology Security Evaluation Criteria (ITSEC)* [2]. Version 1 was published in June of 1990, with a second version released in June of 1991.

The ITSEC does not specify security requirements for specific IT systems.[1] Instead, it provides a framework within which specific IT security requirements can be defined. The ITSEC defines two distinct evaluation criteria: *functionality* and *assurance*.

Functionality requirements are the technical security features (referred to as "security enforcing functions") that are implemented in an IT system in order to support the system's requirements for the maintenance of confidentiality, integrity, and availability. The ITSEC defines ten example functionality classes: F1, F2, F3, F4, F5, F6, F7, F8, F9, and F10. Functionality classes F1 - F5 are roughly equivalent to the TCSEC classes C1, C2, B1, B2, and B3.[2] Functionality classes F6 - F10 represent integrity, availability, data communications integrity, data communications confidentiality, and data communications confidentiality and integrity, respectively.

Assurance requirements provide confidence to the customer of the system as to how well the functionality has been implemented. The ITSEC considers assurance to be a combination of *correctness* (of the security enforcing functions) and *effectiveness* (of these functions). The evaluation levels range from E0 (no confidence) through E1, E2, E3, E4, E5, and E6 (the highest level of assurance). These ratings correspond roughly to the TCSEC D, C1, C2, B1, B2, B3, and A1 levels respectively. Assurance is measured as a combination of a *correctness* rating and a judgement as to the *effectiveness* of the security enforcing functions.

The ITSEC describes an approach for specifying and justifying the security functionality and the level of assurance (i. e., a combination of a correctness level and a judgement of effectiveness) required in a particular system.

1.1.3 Security Requirements in the Commercial Sector

Recognizing that the TCSEC was a valuable starting point, but not sufficient for their security needs, two commercial companies--Bellcore and American Express Travel Related Services (TRS)--independently initiated efforts to develop security requirements for their environments. At Bellcore, these efforts resulted in a *Bellcore Standard Operating Environment Security Requirements* [3] document and at American Express, the efforts resulted in the internal *C2-Plus* company security standard.

---

[1] The ITSEC distinguishes between "products" and "systems" with "products" representing the building blocks from which "systems" are built. A "target of evaluation (TOE)" (as described by the ITSEC) may be either a "system" or a "product." A "system" may be built from approved "products" that were themselves individual TOEs. Since the MSR specifies security requirements for an operating system, it frequently refers to the "product" it is defining as a "system." However, in ITSEC terminology, the MSR TOE is a "product" that can be used in building a "system."

[2] There is no F functionality class equivalent to the TCSEC level A1 since the functionality of B3 and A1 are identical; the difference between B3 and A1 is in the level of assurance, with A1 being higher.

The Bellcore document was developed to meet the security needs of Bellcore and its client companies, the Regional Bell Operating Companies (RBOCs). The requirements specified in the Bellcore document were derived both from commonly recurring security requirements for RBOC computer applications and from experiences of Bellcore's computer security assessment group.

In developing the *C2-Plus* document, TRS found that, while the TCSEC met many requirements of the commercial sector, the prescribed features at the C2-level (and its F2-level counterpart in the European standards) fell short in several areas that were either introduced at higher TCSEC-levels or were not addressed at all. Consequently, the TRS document was developed as an enhanced, commercialized version of the TCSEC C2-level.

Using the TRS document as the base document, the *Commercial International Security Requirements (CISR)* [4] was developed by the International Information Integrity Institute (I-4), a consortium of large international corporations. Part of the rationale for the development of the CISR was that:

> "Military-oriented information security requirements (i. e., TCSEC) are not suitable in many respects for the needs of international businesses." [4]

The final version of the CISR was published in April 1992.

1.1.4 System Security Study Committee

The System Security Study Committee was formed in 1988 in response to a request from the Defense Advance Research Projects Agency (DARPA) to address the security and trustworthiness of U.S. computing and communications systems. The Committee, composed of 16 individuals from industry and academia including computer and communications security researchers and practitioners and software engineers, was charged with developing a national research, engineering, and policy agenda to help the U.S. achieve a more trustworthy computing technology base by the end of the century. In 1991, the Committee published the *Computers at Risk - Safe Computer in the Information Age* [5] report, which presents the Committee's assessment of key computer and communications security issues and its recommendations for enhancing the security and trustworthiness of the U.S. computing and communications infrastructure.

The development of the MSR was guided by one of the recommendations from this report that:

> "...a basic set of security-related principles for the design, use, and management of systems that are of such broad applicability and effectiveness that they ought to be a part of any system with significant operational requirements" [5]

be developed.

1.1.5 Federal Criteria Project

As a result of the Computer Security Act of 1987 [6], NIST was assigned responsibility "for developing standards and guidelines for Federal computer systems ... drawing on the technical advice and assistance ... of the National Security Agency, where appropriate." In addition, NIST was "authorized to assist the private sector, upon request, in using and applying the results of the [NIST-initiated] programs and activities under the" Act. In 1991 (as mentioned previously), NIST and NSA established a working agreement to develop a new FIPS for Trusted Systems Technology called the Federal Criteria for Information Technology Security (FC).

One of the first tasks addressed by the Federal Criteria Working Group was the development of a framework within which distinct sets of security requirements intended to meet the protection needs of varied interest groups can be specified. This framework is referred to as a *Protection Profile*. A Protection Profile "describes generic protection needs"; it is "product independent, describing a range of systems that could meet this same need." Finally, a Protection Profile addresses the following: *Rationale*, *Functionality*, and *Assurance*.

The *Rationale* includes the following: (1) the intended use of products built to meet the protection profile, (2) the assumed environment within which products built to meet the protection profile will operate, and (3) the threats that the protection profile is intended to counter.

The *Functionality* describes the security features that must be provided by a system built to meet the protection profile.

The *Assurance* describes assurance requirements levied on the vendor building a product to meet the protection profile and on the product's evaluations. Two types of assurance requirements are defined: development assurance requirements and evaluation assurance requirements.

1.1.6 Minimum Security Requirements

As noted in Section 1.1, one of the objectives of the Federal Criteria Project is replacement of the TCSEC with a second generation iteration. As the first step of satisfying that objective, the MSR Working Group was tasked with developing a Protection Profile that described an enhanced C2-like class of requirements intended to satisfy the most common security needs of computer system users. The MSR are the NIST effort to satisfy this objective. Much of the MSR are derived from the TCSEC, the ITSEC, the *Bellcore Standard Operating Environment Security Requirements* and the CISR with overall guidance from the *Computers at Risk* report.

The MSR form the basis of one of the protection profiles of volume II of the preliminary Federal Criteria FIPS, the CS2, as mentioned in section 1.1. It is hoped that this Protection Profile, if widely accepted, will form the basis for mutual recognition of system evaluations between nations.

1.2 SCOPE OF THE MSR

The MSR specify computer-based protection mechanisms for the design, use, and management of information systems. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems. The MSR provide administrators of an MSR-conformant computer system with the tools to control the sharing of information and resources based primarily on the identity of users, but also on the time of day, terminal location, or type of access requested by users. The technical measures also provide tools to protect both against common user actions that may compromise security and against deliberate penetration attempts by "crackers". In addition, there are requirements that a conformant computer system provide a tailorable ability to log events that may impact the security of either the system or the information that it is processing.

Systems conforming to this Protection Profile are intended to be useful to a broad base of users, including those in commercial, civil government, and national defense environments. Recognizing that IT product vendors operate in an international marketplace, this Profile has been built to complement international efforts, such as the ITSEC and International Standards Organization (ISO) initiatives.

This Protection Profile specifies "baseline" requirements that constitute generally accepted security expectations for multi-user operating systems. These requirements apply commonly to multi-user workstations, minicomputers, and mainframes. Most required mechanisms are specified to be configurable so that individual customers can satisfy their unique security policies and objectives.

The intent of this Protection Profile is to promote the wide availability of products possessing security enforcing functions that are of such broad applicability and effectiveness that they become part of the "normal" operational requirements of all multi-user operating systems.

1.3 AUDIENCE

These requirements are targeted at three distinct audiences: users, vendors, and evaluators.

Users

The MSR address the basic security needs of general-purpose computer operating systems users. This includes application developers, end users, and administrators in the private, civil and defense government sectors. The requirements focus on the basic security requirements of most commercially available multi-user operating system. All functionality requirements are based on existing and well understood security practices. It is hoped that this set of security requirements will set a basic level of expectation within the user community for the security of the operating systems they purchase.

Vendors

This document provides vendors with a single, well-defined set of security requirements that can be accepted across their entire customer base. These requirements represent the integration of a number of security requirement specifications from various sources into a single set that is expected to have very wide acceptance. Vendors can more confidently use this set to focus on a single system offering what will meet the needs of a significant customer base. The level of detail provided by these requirements should help clarify what the vendor must do to comply.

Evaluators

This document provides product and system evaluators, certifiers, and accrediters with a well-defined set of security requirements. The detailed level of the requirements significantly decreases the need for evaluator interpretation. It is hoped that the similarity of the MSR format to the ITSEC Security Target format will provide a basis for international acceptance that can help lead to mutual recognition of evaluations.

1.4 TERMINOLOGY

The following terminology is used throughout this document:

Requirement: Feature or function that is necessary to satisfy the needs of a typical commercial or government organization. Failure to meet a Requirement may cause application restrictions, result in improper functioning of the system, or hinder operations. A Requirement contains the word *shall* and is identified by the letter "R" in parentheses: (R)

Advisory: Feature or function that may be desired by a typical commercial or government organization. An Advisory represents a goal to be achieved. An Advisory may be reclassified as a Requirement at some future date. An Advisory contains the word *should* and is identified by the letter "A" in parentheses: (A)

1.5 DOCUMENT ORGANIZATION

The MSR is divided into four sections and includes an Appendix, a Glossary and References. Section 1, Introduction (this section), provides introductory and background information. Section 2, Rationale, provides rationale to support the MSR Protection Profile. This includes descriptions of the intended use of the system, the environmental assumptions that were made for an MSR-compliant system, and the expected threats. Section 3, Functionality Requirements, specifies the security functionality that an MSR-compliant system is required to provide. Section 4, Assurance Requirements, specifies the assurances that an MSR-compliant system is required to provide. The Appendix provides a threat analysis, which describes how each threat (identified in Section 2) is

countered. The list of documents in the References section acted as guides, inspiration, or information in preparing this document. Those referenced have a square bracket around a number ([]). The Glossary defines key terms and acronyms used throughout the document. The reader will note that the first occurrence of any term defined in the Glossary has been underlined as an aid to the reader.

2. RATIONALE

This section provides information for prospective purchasers of an MSR-conformant IT system. This information is to aid the purchaser in deciding whether the system will satisfy their security objectives. Specifically, it discusses how the system is intended to be used, the assumptions about the environment in which the system is intended to operate, the threats within that environment, and the security features and assurances that are intended to counter these threats.

2.1 INTENDED METHOD OF USE

A product designed to meet this Protection Profile is intended to be a general purpose, multi-user operating system that runs on either a workstation, minicomputer, or mainframe. This system is expected to support a variety of applications and may support application software development. These applications are for commercial as well as government environments.

Such an MSR-conformant operating system is intended to be used to control access to information based on the identity of individual users or groups of users. The information may be unclassified, sensitive-but-unclassified, or single-level classified, but it may not be multi-level classified information. Such a system is not intended to be used to control access to information at multiple classification levels based on the clearance of the user.

2.2 ENVIRONMENTAL ASSUMPTIONS

The following specific environmental conditions have been assumed in specifying this Protection Profile:

a. The hardware base (e.g., CPU, printers, terminals, etc.) will be protected from unauthorized physical access.

b. There will be one or more personnel assigned to manage the system, including the security of the information it contains.

c. If a network interface is supported, the attached networks will provide some facility to independently confirm the claimed identity of remote machines.

d. The operational environment will be managed according to the operational environment documentation that is required in the Assurance Requirements Section of this protection profile.

2.3 EXPECTED THREATS

A MSR-conformant system is intended to be a "reasonable first-line of defense" against an unauthorized user's attempt to gain access to the system or against an authorized user's inadvertent attempt to gain access to information for which he or she has not been granted access.

It should be understood that highly-motivated attackers, willing to apply the necessary level of effort, may be able to circumvent the security features of the system. These features are not expected to completely eliminate the threat from malicious users or software, such as computer viruses or Trojan Horses.

The following threats have been assumed in specifying this protection profile:

a. An unauthorized user may attempt to gain access to the system.

b. An authorized user may attempt to gain access to resources for which he or she is not allowed access.

c. Security relevant actions may not be traceable to the individual associated with the event.

d. The system may be delivered, installed, or used in an unsecured manner.

e. Data transmitted over a public or shared data network may be modified either by an unauthorized user or because of a transmission error or other communication-related error.

f. Security breaches may occur because available security features are not used or are used improperly.

g. Users may be able to bypass the security features of the system.

h. Users may be denied continued accessibility to the resources of the system (i.e., denial of service).

2.4 SECURITY FEATURES AND ASSURANCES

This section summarizes the security features and assurances that are required to counter the threats discussed in Section 2.3. Detailed requirements for these features and assurances may be found in Sections 3 and 4, respectively, of this protection profile.

2.4.1 Identification and Authentication

An MSR-conformant operating system provides the capability to establish, maintain, and protect a unique identifier for each authorized user. The system also provides the capability to establish, maintain, and protect from unauthorized access information that can be used to authenticate the association of a user with that identifier.

These features are intended to counter the threat that an unauthorized user may attempt to gain access to the system or the information it contains. It also intends to counter the threat that an authorized user may attempt to gain access to resources for which he or she is not allowed access.

2.4.2 Access Control

An MSR-conformant operating system provides the capability for a privileged user, such as a System Administrator, to establish, maintain, and protect from unauthorized access information that defines the identities of users and conditions under which users may access the system. These conditions may include controls based on user identification, time, location, and method of access. The system is also required to display to each user attempting access a warning about unauthorized attempts to access the system. This feature is intended to counter the threat that an unauthorized user may attempt to gain access to the system or the information it contains.

The system provides the capability for an authorized user to specify and control access to information that he or she owns. By default, the system protects newly-created information. Furthermore, once information is deleted, it is not available to subsequent users. This feature is intended to counter the threat that an authorized user may attempt to gain access to resources for which he or she is not allowed access.

The system is designed so that security features can be easily implemented, operated and maintained. This is intended to counter the threats that the system may be delivered, installed, or used in an unsecured manner and that security breaches may occur because available security features are not used or are used improperly.

2.4.3 Audit

An MSR-conformant operating system creates, maintains, and protects a security audit trail, which provides individual user accountability and contains information sufficient for after-the-fact investigation of loss or impropriety.

This feature is intended to counter all of the threats discussed in Section 2.4.2 in the event that the system's access control features have failed to deny unauthorized access.

2.4.4 System Integrity

An MSR-conformant operating system continuously protects itself from users changing or circumventing the security functionality it provides.

This is intended to provide assurance that the security features of the system operate as expected. This is also intended to counter the threats that security breaches may occur because available security features are not used or are used improperly, that users may be able to bypass the security features of the system or that users may be denied continued accessibility to the resources of the system.

2.4.5 Data Integrity

An MSR-conformant operating system protects the consistency and integrity of information.

This is intended to provide assurance that the security features of the system operate as expected. This is also intended to counter the threats that security breaches may occur because available security features are not used or are used improperly, that users may be able to bypass the security features of the system or that users may be denied continued accessibility to the resources of the system.

2.4.6 Reliability of Service

A MSR-conformant system provides the capability to detect and recover from any discontinuity of service, using some combination of automatic and procedural techniques.

This capability is intended to counter the threat that users may be denied continued accessibility to the resources of the system.

2.4.7 Product Development Assurance

A MSR-conformant system has been designed, implemented, and tested to ensure that it meets acceptable minimum security assurance requirements. Specifically, the system has not be designed with any mode of access that would violate or bypass the minimum security functionality requirements of the product.

This is intended to provide assurance that the security features of the system operate as expected. This is also intended to counter the threats that security breaches may occur because available security features are not used or are used improperly, that users may be able to bypass the security features of the system or that users may be denied continued accessibility to the resources of the system.

2.4.8 Product Documentation Assurance

A MSR-conformant system provides documentation to support the secure installation, operation, administration, and use of the product.

This documentation is intended to counter the threat that a system may be delivered, installed, or used in an unsecured manner. This is also intended to counter the threat that security breaches may occur because available security features are not used or are used improperly.

3. FUNCTIONALITY REQUIREMENTS

This section provides detailed functionality requirements[3] that must be satisfied by an MSR-compliant system.

3.1 IDENTIFICATION AND AUTHENTICATION

In this document, the term "user" refers to an individual human or a remote system able to access the target system to which these requirements apply. The identification and authentication process begins the user's interaction with the target system. First, the user supplies a unique identifier (userID) to the system. Then, the user is asked to authenticate that claimed identity by the system. The requirements for identification are presented in the first subsection. The requirements for authentication are presented in the subsequent subsection.

3.1.1 Identification

A userID represents a user uniquely. The userID is used for both access control and accountability. Therefore, the proper maintenance and control of the identification mechanism and the identification databases are vital to system security. The requirements that follow support identification.

Requirements:

1. The system shall use userIDs to identify users. (R)

2. The system shall require users to identify themselves with their unique userIDs before the user is allowed to perform any actions on the system. (R)

3. The system shall internally maintain the identity of all active users (i.e., users currently logged on). (R)

    a. Every process running on behalf of a user shall have associated with it the identity of that user. That is, if the process is invoked by a user, it shall have the userID of that user associated with it. If a process is invoked by another process (that was invoked by the user), the invoked process shall have the userID associated with the invoking process, and so on. (R)

    b. Every process running "autonomously" (i.e., without user invocation), such as print spoolers, database management system servers, and transaction processing

[3] Key terms that have been defined in the Glossary are underlined the first time they are used.

monitors, shall have associated with it an identification code indicating system ownership or a unique process identification code. (R)

4. The system shall provide a mechanism to administratively disable userIDs. This mechanism shall provide an option for automatic re-enabling of disabled userIDs after a customer-specifiable period of time. The use of this mechanism shall require privilege. (R)

5. The system shall automatically disable userIDs after a period of time during which the userID has not been used. The time period shall be customer-specifiable, with a default of sixty days. (R)

6. The system shall provide a mechanism to administratively re-enable or delete disabled userIDs. The use of this mechanism shall require privilege. (R)

7. The system shall provide a mechanism to obtain the status of any userID. (R)

8. The system shall provide a mechanism that allows a collection of userIDs to be referenced together as a group. (R)

   a. A userID shall be able to be associated with more than one group. (R)

   b. The system shall provide a mechanism to modify the group membership of a userID. The use of this mechanism shall require privilege. (R)

   c. The system shall provide a mechanism to list the names of all groups. (R)

   d. The system shall provide a mechanism to list the membership of any group. (R)

9. For those systems that have the architecture to support multiple logons per userID, the system shall provide a mechanism that limits the number of multiple logon sessions for the same userID. The mechanism shall allow limits for userIDs and groups to be specified. The system-supplied default shall limit each userID to one simultaneous logon session. The use of this mechanism shall require privilege. (R)

10. If the system provides a mechanism by which the userID associated with a process can be changed while the process is active, then it shall also provide a mechanism for limiting the userIDs that may change to a userID that would provide any additional privileges. (R)

11. The system shall provide a mechanism to associate customer-specifiable information (e.g., user name and affiliation) with each userID. The use of this mechanism shall require privilege. (R)

3.1.2 Authentication

Once a user has supplied an identifier to the system, the system must verify that the user really corresponds to the claimed identifier. This is done by the authentication mechanism as described by the following requirements. Because passwords are the most commonly used authentication mechanism, a subsection on password requirements follows this section.

Although authentication and system access control processes are often combined for stand-alone systems, the mixing of these processes is less appropriate for distributed or client/server systems. An authenticated user may not have access to every host in a distributed system and may not be allowed direct access to a server. Therefore, this document treats system access control and authentication separately. System access control is in Section 3.2.1.

Note: Network-related issues of authentication (such as proxies and cascading trust) are beyond the scope of this document.

Requirements:

1. The system shall provide a mechanism to authenticate the claimed identity of a user. (R)

2. The system shall appear to perform the entire user authentication procedure even if the userID that was entered was not valid. Error feedback shall contain no information regarding which part of the authentication information is incorrect. (R)

3. The system shall provide a mechanism to support the initial entry or modification of authentication information. (R)

4. The system shall be able to incorporate and use customer-supplied alternative authentication mechanisms, such as token-based cards, biometrics, or trusted third-party techniques, in place of or in addition to the system-supplied authentication mechanism. (R)

    a. If multiple authentication mechanisms are provided, the system shall also provide a separate mechanism to specify the authentication mechanism or mechanisms to be used for specific userIDs and groups. The use of this separate mechanism shall require privilege. (R)

5. The system shall require a privilege to access any internal storage of authentication data. (R)

a. Authentication data transmitted over public or shared data networks should be encrypted.[4] (A)

6. The system shall support an application program interface to an authentication mechanism. (R)

7. If the system provides network access (e.g., dial-in, X.25, or INTERNET), then it shall also provide at least a Class 2 authentication mechanism (as defined in Draft International Standard (DIS) 10181-2 [7]) that can be used at the customer's discretion. The networking software shall be able to be disabled or configured out of the system. (R)

3.1.2.1 Password Requirements

Although systems are not required to use passwords as the user authentication mechanism, passwords are still the most commonly used mechanism for authentication. Extensive experience with password mechanisms has led to a solid understanding of what constitutes good password management. The following requirements capture this understanding.

Note: These requirements apply only to systems using passwords. Other authentication methods, such as token-based authentication, cryptographic-based authentication, and biometrics, are beyond the scope of this document.

Requirements:

1. The system shall provide no mechanism whereby a single stored password entry is explicitly shared by multiple userIDs. The system shall provide no means to facilitate the sharing of passwords by multiple users. (R)

2. The system shall allow a user to choose a password that is already associated with another userID. The system shall provide no indication that a password is already associated with another userID. (R)

3. The system shall store passwords in a one-way encrypted form. (R)

   a. The system shall require privilege to access encrypted passwords. (R)

   b. Unencrypted passwords shall be inaccessible to all users. (R)

---

[4] Since encryption algorithms are subject to national export control, statements specifying data encryption have been stated as advisories rather than requirements. This will allow the data encryption mechanism to be packaged by the vendor as a separate option and not "bundled" into the baseline system.

4. The system shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device. (R)

5. The system shall, by default, prohibit the use of null passwords during normal operation.[5] (R)

6. The system shall provide a mechanism to allow a user to change his or her password. This mechanism shall require re-authentication of the user identity. The system shall provide a mechanism to set or initialize passwords for users. The use of this mechanism shall require privilege. (R)

7. The system shall enforce password aging on a per-userID or per-group basis (i.e., a user shall be required to change his or her password after a customer-specifiable minimum time). The system-supplied default for all non-privileged users shall be sixty days. (R)

    a. The system-supplied default for those userIDs that may acquire privileges shall be thirty days. (R)

    b. After the password aging threshold has been reached, the password shall no longer be valid. (R)

8. The system shall provide a mechanism to notify users in advance of requiring them to change their passwords.[6] This can be done by either:

    a. Notifying users a customer-specifiable period of time prior to their password expiring. The system-supplied default shall be seven days. (R)

    or

    b. Upon password expiration, notifying the user but allowing a customer-specifiable subsequent number of additional logons prior to requiring a new password. The system-supplied default shall be two additional logons. (R)

---

[5] A capability, accessible only to a privileged user, to allow null passwords during system logon on a per-userID or per-port basis may be provided.

[6] Users are notified in advance so that they have time to think of a replacement password.

9. Passwords shall not be reusable by the same userID for a customer-specifiable period of time. The system-supplied default shall be six months.[7] (R)

10. The system shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

    a. Passwords shall meet a customer-specifiable minimum length requirement. The system-supplied default minimum length shall be eight characters. (R)

    b. The password complexity-checking algorithm shall be modifiable by the customer. The system-supplied default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character. (R)

    c. The system should provide a mechanism that allows customers to specify a list of excluded passwords (e.g., company acronyms, common surnames). (A)

        (1) The system should prevent users from selecting a password that matches any of those on the list of excluded passwords. (A)

11. If system-supplied password generation algorithms are present in the system, they shall meet the following requirements:

    a. The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable or pass-phrases). (R)

    b. The system should give the user a choice of alternative passwords from which to choose. (A)

    c. Passwords shall be reasonably resistant to brute-force password guessing attacks (i.e., the total number of system-generated passwords shall be of at least the same order of magnitude as what a user could generate using the rules specified in requirement 10 above). (R)

    d. If the "alphabet" used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet. (R)

---

[7] Since the MSR does not require a minimum time period to elapse between password changes, the reuse requirements have not been based on the number of subsequent password choices.

e. The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity). (R)

12. The system shall provide a mechanism by which a data entry/display device may force a direct connection between the port to which it is connected and the authentication mechanism.[8] (R)

3.2 ACCESS CONTROL

Access control determines what an authenticated user can do with the system. Two types of access control are considered here: system access and resource access. The requirements for system access control are presented in the first subsection. The requirements for resource access control are presented in the subsequent subsection.

3.2.1 System Access Control

Once a user is authenticated, a check is made to see if the user is allowed to access the system. The qualifying checks for system access can include time-of-day, day-of-week, date, location of terminal, or means of access (e.g., dial-up port or local area network port).

The requirements for system access control follow.

Requirements:

1. The identity of all users shall be authenticated before access is granted to any resources or system information. (R)

   a. The system shall provide no userIDs that permit unauthenticated system access during normal system operation. (R)

   b. The system should authenticate remote machines during the establishment of an inter-system association. (A)

2. The system shall provide a mechanism to authorize users to access the system, revoke users from accessing the system, and modify the security information associated with users. The use of this mechanism shall require privilege. (R)

---

[8] In the case of a user directly connected to the system on a local terminal, this requirement ensures that the user is in direct communication with the system, thus providing a defense against "spoofing" attacks.

a. The system shall allow access to only those users who are authorized to access the system. (R)

b. The system shall provide a mechanism that lists all users who are authorized to access the system. The use of this mechanism shall require privilege. (R)

3. The system shall provide a mechanism for user-initiated locking of interactive sessions (e.g., keyboard locking) that includes:

a. Requiring user authentication prior to unlocking the session (R)

b. Disabling all data entry/display devices from any activity other than unlocking the session (R)

c. Clearing or over-writing the display to make its current contents unreadable (R)

4. For interactive sessions, the system shall lock the session after a customer-specifiable period of user inactivity. The system-supplied default shall be fifteen minutes. (R)

a. The system shall provide a mechanism to specify that sessions be terminated rather than locked after a period of inactivity. The use of this mechanism shall require privilege. (R)

5. The system logon procedure shall exit and end the attempted session if the user authentication procedure is incorrectly performed a customer-specifiable number of times. The system-supplied default shall be three times. (R)

a. The system shall generate an alarm when this threshold is exceeded. (R)

b. When the above threshold has been exceeded, a customer-specifiable interval of time shall elapse before the logon process can be restarted on that data entry/display device. The system-supplied default shall be sixty seconds. (R)

(1) The system should increment the time interval on successive violations. (A)

c. The system shall provide a mechanism to disable the userID when this threshold is exceeded. (R)

(1) By default, this mechanism shall be disabled. (R)

6. The system shall provide a mechanism to allow or deny specified userIDs to access the system during specified ranges of time. The use of this mechanism shall require privilege. The ranges shall include:

a. Time-of-day (R)
b. Day-of-week (R)
c. Calendar date (R)

7. The system shall provide a mechanism to allow or deny specified userIDs to access the system based on means of access or port of entry. The use of this mechanism shall require privilege. (R)

   a. The system shall provide a mechanism to specify the userIDs authorized to access the system via dial-up facilities. The use of this mechanism shall require privilege. (R)

   b. The system shall provide a mechanism to specify the userIDs authorized to access the system via network facilities. The use of this mechanism shall require privilege. (R)

8. The system shall provide a mechanism to limit the privilege a user may obtain based on means of access or port of entry. The use of this mechanism shall require privilege. (R)

9. If the system provides network access, then it shall also provide a mechanism to end an abnormally terminated session such that a new user does not have access to a previous user's session. (R)

10. Prior to initiating the system logon procedure, the system shall display an advisory warning message to the user regarding unauthorized use of the system and the possible consequences of failure to heed this warning. (R)

    a. The message shall be customer-specifiable. (R)

    b. The system shall be able to display a message of up to twenty lines in length. (R)

    c. The following message shall be displayed by default:

       NOTICE: This is a private computer system. Unauthorized access or use is prohibited and may lead to prosecution. (R)

11. Upon a user's successful access to the system, the system shall display the following to the user and shall not remove it without user intervention:

    a. The date, time, and means of access or port of entry of the user's last successful system access. (R)

b. The number of unsuccessful attempts to access the system since the last successful system access by that userID. (R)

3.2.2 Resource Access Control

Once the user has been granted access to the system as a whole, the question of which resources that authenticated user may access still remains. An owner, or a privileged user, uses provided mechanisms to allow or deny other users accesses to that resource. The requirements below support resource access control.

The additional requirements for protection of data in de-allocated resources are presented in the subsection on object reuse.

Requirements:

1. The system shall control access to all resources. (R)

2. The system shall control access to resources based on authenticated userIDs. (R)

3. For each resource, the system shall provide a mechanism to specify a list of userIDs or groups with their specific access rights to that resource (i.e., an access control list). (R)

   a. The access rights that may be specified shall, at a minimum, include "read," "write," and "execute-only." (R)

      (1) There should be separate "create" and "delete" access rights for modification of entries in directories or catalogs. (A)

      (2) The system should support the explicit denial of all access rights to a userID or group. (A)

   b. The access rights associated with a userID shall take precedence over the access rights associated with any groups of which that userID is a member. (R)

   c. For systems where a userID can be an active member of multiple groups simultaneously, if any group entry allows an access right for that userID, then the userID is allowed that right (subject to "b" above). (R)

   d. The system shall provide a mechanism to specify default access rights for userIDs not otherwise specified either explicitly by userID or implicitly by group membership. (R)

4. A userID's access rights to a resource shall be checked, at a minimum, when access to that resource is initiated. (R)

5. The system shall provide a mechanism to specify the owner(s) of the resource (i.e., the user(s) who can modify the contents of a resource's access control list). The use of this mechanism shall be limited to current owner(s) and user(s) with privilege. (R)

    a. There should be a distinct access right to modify the contents of a resource's access control list (e.g., an "ownership" or "control" access right). (A)

6. The system shall provide a mechanism to modify the contents of a resource's access control list. The use of this mechanism shall be limited to owner(s) and user(s) with privilege. (R)

7. The system shall provide a mechanism to specify the default contents of the access control list of a newly created resource. The system-supplied default contents shall specify that only the creator of the resource has any access rights. (R)

8. The system should provide a mechanism to control access to resources based on the following. The use of this mechanism should be limited to the owner(s) of the resource and users with privilege:

    a. Means of access or port of entry (A)
    b. Time-of-day (A)
    c. Day-of-week (A)
    d. Calendar date (A)
    e. Specific program used to access the resource. (A)

9. The system shall provide a mechanism to identify all resources in the system that are owned by a specified userID, the resources to which that userID is allowed access, and the specific access right(s) for each resource. The use of this mechanism shall require privilege. (R)

10. The system shall provide a mechanism to deny specific access rights to all resources for specified userIDs or groups. This mechanism shall override the standard resource access control mechanisms. The use of this mechanism shall require privilege. (R)

11. Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource. (R)

12. The system shall protect all information used for resource access control decisions (e.g., access control lists, group lists, system date and time). (R)

3.2.2.1 Object Reuse

Resources owned by a user or by the system are de-allocated when no longer needed, but data left in these de-allocated resources continues to be protected from disclosure. This protection is the purpose of the requirements for object reuse that follow.

Requirements:

1. The system shall ensure that users who do not possess an appropriate privilege are not able to access the contents of a resource that has been returned to the system after use. (R)

2. The system shall ensure that a user is not able to access the prior contents of a resource that has been allocated to that user by the system. (R)

3.2.3 Privileges

A privilege enables a user to perform a security relevant operation or a command that, by default, is denied to that user. Privileges must be tightly controlled, and users with privilege must be accountable for security relevant actions. The requirements supporting the privilege mechanism follow.

Requirements:

1. The system shall support a privilege mechanism that meets the following requirements:

    a. Separate privileges shall be associated with groups of related security relevant operations or commands. (R)

        (1) Separate and distinct privileges should be associated with distinct security relevant operations. (A)

        (2) Privileges that permit overriding or bypassing the access control mechanisms should be separate and distinct from any and all other privileges. (A)

    b. A user shall be assigned a privilege in order to invoke the corresponding operation. (R)

        (1) There should be an application program interface that allows an application with privilege to dynamically assign privileges to itself. (A)

2. The system shall provide a mechanism to associate privileges with userIDs. The use of this mechanism shall require a separate and distinct privilege. (R)

3.3 AUDIT

Audit supports accountability by providing a trail of user actions. Actions are associated with individual users for all security relevant events and are stored in an audit trail. This audit trail can be examined to determine what happened and what user was responsible for a security relevant event. The audit trail data must be protected from unauthorized access, modification, or destruction. In addition, the audit trail data must be available in an easily readable form and in a timely manner for analysis. The requirements for data recording are presented in the first subsection. The requirements for data reporting are presented in the subsequent subsection.

3.3.1 Data Recording

Audit data is recorded from several sources (such as the logon host's operating system or a remote application) to produce a complete picture of a user's security relevant actions. Therefore, audit data must be correlated across audit collection systems. The mechanisms providing audit data recording must be tailorable to each system's needs. Both the audit data itself and the mechanisms to determine what audit data is recorded are protected by privileges. The requirements below support data recording.

Requirements:

1. The system shall provide a mechanism for generating a security audit trail that contains information to support after-the-fact investigation of loss or impropriety and appropriate management response. The system shall support an application program interface that allows an application with privilege to append data to the security audit trail or to an applications-specified alternative security audit trail. (R)

2. The system shall provide end-to-end user accountability for all security relevant events. The user identification information associated with any system request or activity shall be maintained and passed on to any other connected systems so that the initiating user can be made accountable for the lifetime of the request or activity. (R)

3. The system shall protect the security audit trail from unauthorized access. (R)

    a. Maintenance and management of the security audit trail files shall require privilege. (R)

    b. The system should support an option to maintain the security audit trail data in encrypted format.[9] (A)

---

[9] See footnote 4.

4. The system shall provide a mechanism to dynamically control, during normal system operation, the types of events recorded. This mechanism shall include selective disabling of the recording of default audit events and the enabling and disabling of other events. The use of this mechanism shall require privilege. (R)

    a. It shall not be possible to disable the recording of activities that require privilege. (R)

    b. The system shall record any modification to the set of audited events. (R)

5. The system shall protect the audit control mechanisms from unauthorized access. (R)

6. The system shall, by default, cause a record to be written to the security audit trail for at least each of the following events:

    a. Failed user authentication attempts (R)

    b. Resource access attempts that are denied by the resource access control mechanism (R)

    c. Attempts, both successful and unsuccessful, to obtain privilege (R)

    d. Activities that require privilege (R)

    e. Successful accesses of security-critical resources (R)

    f. Changes to users' security information (R)

    g. Changes to the set of privileges associated with a user (R)

    h. Changes to access rights of resources (R)

    i. Changes to the system security configuration (R)

    j. Modification of system-supplied software (R)

7. The system shall provide a mechanism to enable or disable the recording of other events into the security audit trail. The use of this mechanism shall require privilege. These events shall include, at a minimum:

    a. Successful user authentication attempts (R)

    b. Creation and deletion of resources (R)

c. Disk file access (R)

d. Tape volume or tape file access (R)

e. Program execution (R)

f. On-line command execution (R)

g. Customer-defined events (R)

h. Activities of a specified userID (R)

8. For each recorded event, the audit record shall identify, at a minimum:

   a. Date and time of the event (R)

   b. UserID and associated point of physical access (e.g., terminal, port, network address, or communication device) (R)

   c. Type of event (R)

   d. Names of resources accessed (R)

   e. Success or failure of the event (R)

9. The character strings input as a response to a password challenge shall not be recorded in the security audit trail. (R)

10. The audit control mechanism shall provide an option to enable or disable the recording of invalid userIDs during failed user authentication attempts. (R)

11. Audit control data (e.g., audit event masks) shall survive system restarts. (R)

12. The system shall provide a mechanism for automatic copying of security audit trail files to an alternative storage area after a customer-specifiable period of time. (R)

13. The system shall provide a mechanism for automatic deletion of security audit trail files after a customer-specifiable period of time. It shall be possible to disable this mechanism. The system-supplied default shall be thirty days. (R)

14. The system shall allow site control of the procedure to be invoked when audit records are unable to be recorded. Options provided to handle this condition shall include:

a. Generate an alarm. This shall be the default action. (R)

b. Initiate secure system shutdown. (R)

15. The system shall provide tools to monitor the activities (i.e., capture the keystrokes) of specific terminals or network connections in real time. The use of these tools shall require a separate and distinct privilege. (R)

3.3.2 Data Reporting

Once the audit data is recorded, it is analyzed and reported. Reporting can be done by reports generated on request, or by alarms generated immediately when security violations are detected. The requirements below support data reporting.

Requirements:

1. The system shall provide a mechanism for reporting alarms. The system shall provide a mechanism for specifying how (e.g., where or to whom) alarms are reported. The use of this mechanism shall require privilege. (R)

2. The system shall provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communications facilities. The use of these tools shall require privilege. (R)

   a. The system shall provide a tool to independently and selectively review the actions of any one or more users, including users with privilege, based on individual user identity. (R)

   b. The system shall provide a tool to produce a report of all occurrences of modifications to any resources. (R)

   c. These tools shall be capable of being run concurrently with normal system operations. (R)

3. The system should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security relevant events that may indicate an imminent security violation. This mechanism should be able to generate an alarm when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system should take the least disruptive action to terminate the event. (A)

3.4 SYSTEM INTEGRITY

Users expect to share computer resources without interference or damage from other users. This is called system integrity. The requirements that follow provide for mechanisms that promote separation of user and system processes and data, protection of software, firmware, and hardware from unauthorized modifications (whether deliberate or accidental), and control of operator and maintenance personnel actions.

Requirements:

1. The system shall separate and protect a user process and its internal data from other user processes. The system's internal programs and internal data shall be separated and protected from any user processes. (R)

2. Mechanisms (e.g., modification dates, checksums, digital signatures) shall exist that make it possible to verify that the currently installed software has remained consistent with the delivered software (i.e., no unauthorized modifications have been made). (R)

3. The system shall restrict the use of:

   a. Privileged instructions (R)

   b. Supervisory state or other privileged hardware states (R)

4. The system shall control and audit the use of any operator consoles. (R)

5. Modification or replacement of the software provided with the system shall require privilege. (R)

6. Execution of system maintenance and repair software shall require privilege. (R)

7. The system shall provide mechanisms that can be used to validate the correct operation of the system. These mechanisms shall address:

   a. Monitoring of system resources (R)

   b. Correct operation of on-site hardware and firmware elements (R)

   c. Corruption of access control information (R)

   d. Detection of communication errors above a customer-specifiable threshold (R)

3.5 DATA INTEGRITY

Users expect data to be entered and maintained in a correct, consistent state. This is called data integrity. This expectation applies to both user data and system data. The requirements that follow provide for mechanisms that promote tracking of changes to resources, and the protection of data against exposure, unauthorized modification or deletion as it is transmitted and while it is stored.

Requirements:

1. The system shall provide a mechanism to determine the date and time a resource was last modified. The use of this mechanism shall be limited to users with access rights to that resource and users with privilege. (R)

2. The system shall provide a mechanism to verify the integrity of data in a resource (e.g., a checksum or digital signature). The system shall provide a mechanism to verify the integrity of information passed across a communication channel. (R)

3. The system should provide an encryption mechanism that can be used to preserve the integrity of data in a resource.[10] (A)

4. The system shall provide a tool for checking file system and storage medium integrity. The system shall execute this tool periodically. (R)

5. The system shall provide a mechanism to generate a status report detailing the values of all parameters and flags that affect the secure operation of the system. The use of this mechanism shall require privilege. (R)

6. If the system command interpreter provides a mechanism for users to control the order of directory/path search for command resolution, then:

    a. System supplied commands shall be executed by default. (R)

    b. The system should allow a user with privilege to revoke user access to this mechanism on a per-userID basis. (A)

3.6 RELIABILITY OF SERVICE

Users expect a quantifiable and reliable level of service from a system. The requirements that follow provide for mechanisms that promote the continuous accessibility and usability of

---

[10] See footnote 4.

resources by an authorized user. These mechanisms also allow prevention or limitation of interference with time-critical operations, and allow the system to maintain its expected level of service in the face of any user action threatening this level, whether the action is deliberate or accidental.

Requirements:

1. The system should detect and report all conditions that degrade service below a customer-specifiable minimum. When possible, the system should isolate and report the source of the condition. (A)

2. The system shall provide a mechanism for controlling consumption of disk space and CPU usage on a per-userID and per-group basis. (R)

3. The system shall provide a mechanism to allow recovery after a system failure or other discontinuity without a security compromise. (R)

4. The system shall provide a mechanism to support software and data backup and restoration. (R)

5. The system shall provide synchronization points (e.g., checkpoint restarts) to facilitate recovery. (R)

4. ASSURANCE REQUIREMENTS

The TCSEC and ITSEC recognize that the presence of security features alone are not sufficient for ensuring a secure product. Underlying the security features must be a process of product development to provide assurance that the security features actually work as claimed and that no security flaws were introduced as a result of the development process. In addition, documentation must be provided that supports the secure installation, operation, administration, and use of the product.

The requirements that constrain the product development process and specify the documentation to be produced are commonly called assurance requirements. The assurance requirements that follow have been included to complete the document. Originally, these requirements were part of the Functionality Requirements.

Section 4.1 presents assurance requirements for the product development process, and Section 4.2 presents the product documentation requirements.

4.1 PRODUCT DEVELOPMENT ASSURANCES

A MSR-conformant system is one that has been designed, implemented, and tested to ensure that it meets acceptable basic security assurance requirements. Specifically, the system has not been designed with any mode of access that would violate or bypass the basic security functionality requirements of the product. The requirements below are intended to provide assurance that the security features of the system operate as expected.

1. Security mechanisms shall be protected from external interference, e.g., modifications to its code or data structures. (R)

4.2 PRODUCT DOCUMENTATION ASSURANCES

A MSR-conformant system provides documentation for users, administrators, and operators to support the secure installation, operation, administration, and use of the product. The requirements for product documentation assurances are intended to ensure that security breaches do not occur because available security features are not used or are used improperly.

The requirements for user documentation are presented in the first subsection. The requirements for administrator and operator documentation are presented in subsequent subsections.

1. Instructions and documentation on security considerations shall be provided separately for users of the system, administrators of the system, and operators of the system. (R)

4.2.1 User Documentation

1. User documentation shall include a description of the security mechanisms that are non-transparent to the user, an explanation of their purpose, and guidelines on their use. (R)

4.2.2 Administrator Documentation

1. Administrator documentation shall include the following:

   a. Cautions about functions and privileges that need to be controlled when running a secure facility. (R)

   b. Documentation on the use of all audit tools. This documentation shall contain:

      (1) Recommended procedures for examining and maintaining the audit trail files. (R)

      (2) Detailed audit record structure for each type of audit event. (R)

      (3) Recommended procedures for periodic backup and deletion of audit trail files. (R)

      (4) Recommended procedures for checking the amount of free disk space available for the audit trail files. (R)

   c. Detailed descriptions of the administrator functions related to security, including adding or deleting a userID, changing the security characteristics of a user, etc. (R)

   d. A description of the basic set of privileges required for an operator and for an administrator. (R)

   e. Recommended procedures for protecting vendor-supplied userIDs. (R)

   f. Recommendations on setting the basic access permissions on all files and directories. (R)

g. Recommendations for running file system or disk integrity-checking utilities on a regular basis. (R)

h. Guidelines on the consistent and effective use of the protection features of the system, how they interact, and how to securely generate a new system. (R)

i. A list of all security parameters that are under administrator control. (R)

j. Recommendations for site security self-assessment techniques, procedures, and reports. (R)

k. Recommendations for password requirements, dial-access restrictions, contingency plans, disaster recovery plans, etc. (R)

l. A section that addresses common intrusion techniques and other threats and procedures for detecting and preventing them. (R)

4.2.3 Operator Documentation

1. Operator documentation shall include the following:

   a. Procedures necessary to initially start, e.g., boot, the system in a secure manner. (R)

   b. Procedures to resume secure system operation after any lapse in system operation. (R)

   c. Recommendations and procedures for running software and data backup and restoration. (R)

APPENDIX

THREAT ANALYSIS

This section provides a description of the requirements that counter the threats identified in Section 2.3.

A.1 AN UNAUTHORIZED USER MAY ATTEMPT TO GAIN ACCESS TO THE SYSTEM.

Identification and Authentication requirements are the principle countermeasure to the threat of unauthorized users gaining access to the system. The MSR focus primarily on passwords for authentication of users.

Passwords, if not properly administered, are considered vulnerable to a threat of an unauthorized user gaining access to the system. For this reason the MSR specify password requirements that promote a strong organizational password management program. These requirements specify a minimum-length password, a password complexity-checking algorithm, as well as an advisory requirement to provide the capability to exclude a list of customer-specified passwords. Such requirements support the use of passwords that are effective against password guessing. To further reduce the probability of a password being guessed, requirements limit the number of attempted guesses that can be made by a user associated with a specific userID. The probability of a single password being guessed is further reduced by requirements for password aging, as well as limitations on password reuse.

The MSR allow for a password generating capability. Because random passwords can be difficult to remember and users are tempted to write them down, requirements are specified for the generation of passwords that are easy to remember (e.g., pronounceable). Additionally, an advisory requirement is specified to allow users to choose from a list of alternative passwords.

In the event a user feels his or her password has been compromised, a requirement allows a user to change the password. Because a password can be compromised by observing the characters on a terminal screen as it is being typed, the clear-text representation of the password on the data entry/display device must be blotted out.

Although passwords are currently the most common method for authenticating users, the MSR support the capability for a variety of authentication mechanisms, such as smart-cards, cryptographic-based authentication, and biometrics. This allows an organizations to acquire and

integrate stronger user authentication capabilities where penetration threats warrant such a capability.

System access control requirements also provide countermeasures to the threat of unauthorized users gaining access to the system. Once a user is authenticated, a check is made to determine if the user is allowed further access to the system. The qualifying checks for system access can include time-of-day, day-of-week, date, location of terminal, or method of access (e.g., dial-up port or local area network port). These requirements provide finer-grained and organization-specific system access control capabilities.

Requirements are specified to display an advisory warning message to all users prior to system logon to discourage a would-be system penetrator from attempting an unauthorized system access. Such a message can also provide a legal basis for subsequent prosecution of system penetrators.

Although not a direct countermeasure, auditing requirements are specified to provide the capability to perform an after-the-fact analysis of unauthorized system access attempts. The MSR specify auditing requirements to monitor failed login attempts. In addition, the MSR specify requirements to display to an authorized user, upon successful system access, the date and time, method of access or port of entry, and the number of failed logon attempts since the last successful system access by his or her userID. These requirements provide an organization with the capability to detect attempted or successful system penetrations. This provides the opportunity for the organization to take corrective action, such as strengthening existing user authentication methods or changing a password.

A.2 AUTHORIZED USERS MAY ATTEMPT TO GAIN ACCESS TO RESOURCES FOR WHICH THEY IS NOT ALLOWED ACCESS.

Authorized users can gain access to resources for which they are not allowed by assuming the userID of another user and gaining the associate access rights. This can be accomplished by exploiting vulnerabilities associated with passwords, or by spoofing legitimate userID authorization prompts and stealing passwords associated with other users. To address the vulnerability associated with passwords, the MSR specify password requirements that promote a strong organizational password management program. In addition to those password requirements described in A.1 to address penetration threats from unauthorized users, other password requirements have been specified to counter the threat of an insider (authorized user) attack. The MSR specify requirements that prohibit the vendor from providing a mechanism that explicitly allows the sharing of a single password by multiple userIDs. If users were allowed to share a single password, there would be no way to prohibit one user from assuming the userID of another user who shared the password and gaining his or her associated access right. In the event that a user selects a password that is already in use by another user, requirements disallow

the system from acknowledging the dual association. To counter the threat of an authorized user creating a spoof of legitimate userID authorization prompts, the MSR specify requirements for a direct communication path between the user and the system.

Once an authorized user has gained access to the system, the threat still remains for gaining access to resources for which he or she is not authorized. At the resource level, the MSR specify access control features to mediate user access to all resources including data, as well as programs and transactions used to manipulate data. These controls are based on userID and mode of access (i.e., read, write). In addition, advisory requirements are specified to provide access controls based on port of entry, time-of-day, day-of-week, calendar date, and specific programs used to access resources. The MSR also specify general authentication facilities for use by application developers, system administrators, or users for the enhanced protection of resources.

The MSR specify requirements to provide users with the capability to lock an interactive session and to clear the content of their screens without having to logoff the system. This reduces the likelihood that a user will leave his or her terminal while engaged in an active session.

The object reuse feature has been specified to ensure that resource contents are cleared before reuse. This reduces the vulnerability that the resource content can be read before it is overwritten.

The MSR specify privilege requirements to allow identification of an individual user and the association of a minimum set of privileges required to perform a single task (e.g., audit log review, password management). Through these requirements, the MSR allow an organization to specify different privileges for different users, depending on what task is required to be performed. Least privilege is particularly important for those systems and organizations where there is a "privileged user" or "superuser" capability that could otherwise grant a wide set of privileges to users that need only a subset of those privileges.

Data and system integrity features are specified to provide protection against an unauthorized or undesired modification of system data. Such features include process isolation and system configuration checks and controls, as well as encryption and checksum facilities for use by application developers, administrators, and general users.

Requirements are specified to display an advisory warning message to all users prior to system logon to discourage unauthorized system use. Such a message can also provide a legal basis for subsequent prosecution.

A.3 SECURITY RELEVANT ACTIONS MAY NOT BE TRACEABLE TO THE INDIVIDUAL ASSOCIATED WITH THE EVENT.

MSR accountability and audit requirements are specified to provide the capability to track security relevant actions performed by users, and link such actions to the responsible user. Audit features are specified to provide post-collection audit analysis on specific data items, users, and communication facilities. In addition, the MSR specify real-time monitoring and reporting of events that may indicate a security violation requiring immediate administrative attention.

A.4 THE SYSTEM MAY BE DELIVERED, INSTALLED, OR USED IN AN UNSECURED MANNER.

This threat is countered in numerous places in the MSR by explicitly requiring that the system be delivered with all security services turned on. This ensures that the system is secure by default rather than insecure by default. This is complemented by allowing many security services to be configured so that, as a specific organization gains experience with the actual threats in its environment, the organization can adjust the degree of security in the system. In addition, there are several requirements that reinforce the "security by default" perspective for initial installation. Finally, one of the primary purposes of security administrative documentation is to increase the likelihood that the administrator will run the system in a secure manner.

A.5 DATA TRANSMITTED OVER A PUBLIC OR SHARED DATA NETWORK MAY BE INTERCEPTED BY AN UNAUTHORIZED USER.

This threat is countered by requirements for authentication, system access control, data integrity, and audit. In addition, requirements to support token-based authentication as well as requirements for network access have been specified to counter the threat of the interception of a user's authentication data. System access control requirements are specified to ensure that a network user is not capable of gaining access to a previous user's session. Requirements for an encryption facility provide the capability to preserve both confidentiality and integrity of data transmitted over a network. The audit requirement provides for audit tools in the event that an attack is mounted and it is necessary to reconstruct the event.

A.6 DATA TRANSMITTED OVER A PUBLIC OR SHARED DATA NETWORK MAY BE MODIFIED EITHER BY AN UNAUTHORIZED USER OR BECAUSE OF A TRANSMISSION ERROR OR OTHER COMMUNICATION-RELATED ERROR.

This threat is countered by requirements for system integrity, data integrity, and audit. System and data integrity requirements provide for mechanisms to detect communication errors and to verify the integrity of information passed across a communication channel. Audit requirements provide for tools that allow reconstruction of the event that resulted in the error after an attack.

A.7 SECURITY BREACHES MAY OCCUR BECAUSE AVAILABLE SECURITY FEATURES ARE NOT USED OR ARE USED IMPROPERLY.

Requirements for authentication, system and resource access control, data integrity, and product documentation provide a basis for countering this threat. Authentication requirements provide for password management procedures to reduce the possibility of easy-to-guess passwords. System access control requirements prohibit default accounts that don't require authentication. Resource access control requirements mandate that the system is delivered with restricted access to resources and that the default access to newly-created resources is limited to the creator. This decreases the chance of setting access too permissively.

Data integrity requirements provide a mechanism for listing all of the system security parameters. This allows a system administrator to confirm that the system is properly configured. Product documentation requirements for user, administrator, and operator documentation describe how to use, administer, and configure the system in a secure manner.

A.8 USERS MAY BE ABLE TO BYPASS THE SECURITY FEATURES OF THE SYSTEM.

This threat is countered by several authentication, access control, audit, and integrity requirements. Authentication requirements protect authentication data from unauthorized users and require that passwords are stored in encrypted form. System access control requirements provide the user with the date, time, and means of access of the user's last successful system access so that unauthorized logons may be detected. Resource access control requirements protect access control data and ensure that users can't scavenge for data.

Audit requirements provide for logging of successful accesses to resources, as well as changes to the system security configuration and system software in the event that the system security features have been bypassed, especially if combined with the advisory requirement for a real-time automated reduction, analysis, and alarm tool. System integrity requirements provide

mechanisms for detecting unauthorized modifications to system software or corruption of access control information, and data integrity requirements provide mechanisms for detecting unauthorized modification of resource data.

A.9 USERS MAY BE DENIED CONTINUED ACCESSIBILITY TO THE RESOURCES OF THE SYSTEM (I.E., DENIAL OF SERVICE).

Reliability of service requirements promote the continued accessibility of system resources by authorized users. These requirements principally counter threats related to intentional or unintentional denial of service attacks. The requirements include detecting and reporting facilities, such as: features to monitor and control the consumption of disk space and CPU usage, controls to limit systematically disabling userIDs, mechanisms for recovery in the event of a system crash, and facilities for software and data backup and restoration.

REFERENCES

[1] U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

[2] Information Technology Security Evaluation Criteria (ITSEC) - Provisional Harmonized Criteria, Version 1.2, June 1991.

[3] Bellcore Standard Operating Environment Security Requirements, TA-STS-001080, Issue 2, June, 1991.

[4] Commercial International Security Requirements (CISR), Cutler, K. and Jones, F., Final Draft, September 9, 1991.

[5] Computers at Risk - Safe Computing in the Information Age, National Research Council, National Academy Press, 1991.

[6] Computer Security Act of 1987, January 8. 1988, P.L. 100-235.

[7] Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 2: Authentication Framework, Draft International Standard DIS 10181-2, International Organization for Standardization, 13 May 1991

These documents are not referenced, but provided guidance, inspiration, or information in preparing this document.

Assessing Federal and Commercial Information Security Needs, Ferraiolo, D., Gilbert, D., and Lynch, N., NISTIR 4976, November 1992.

Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, Willis Ware, Editor, R-609-1, 1970, Reissued October 1979.

Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, International Standard ISO 7498-2, International Organization for Standardization, 1988

GLOSSARY

ACRONYMS

CISR	Commercial International Security Requirements
CSR	Commercial Security Requirements for Multi-user Operating Systems
DARPA	Defense Advance Research Projects Agency
DIS	Draft International Standard
DoD	Department of Defense
FIPS	Federal Information Processing Standard
ISO	International Standards Organization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local area network
MSR	Minimum Security Requirements
NIST	National Institute of Standards and Technology
NSA	National Security Agency
RBOCs	Regional Bell Operating Companies
TCSEC	Trusted Computer System Evaluation Criteria
TRS	Travel Related Services

TERMS

Access Control List. A list of entities, together with their access rights, that are authorized to have access to a resource. [ISO]

Accountability. The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO]

Application Program Interface. A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Authentication. The process of proving the claimed identity of an individual user, machine, software component or any other entity. Typical authentication mechanisms include conventional

password schemes, biometrics devices, cryptographic methods, and onetime passwords (usually implemented with token based cards.)

Authentication Information. Information used to establish the validity of a claimed identity. [ISO]

Authorized. Entitled to a specific mode of access.

Channel. An information transfer path within a system. May also refer to the mechanism by which the path is effected. [TCSEC]

Clear-text. Intelligible data, the semantic content of which is available. [ISO]

Configuration. The selection of one of the sets of possible combinations of features of a system. [ITSEC]

Customer-Specifiable. The features of a MSR-compliant system that are set with a default value by the manufacturer, but can be reset after delivery by the customer to reflect the customer's security policy. These features are usually reset at the time of installation by an administrator or other customer authorized person and cannot be changed without the appropriate privilege at other times.

Group. A named collection of userIDs.

Identification. A unique, auditable representation of identity within the system usually in the form of a simple character string for each individual user, machine, software component or any other entity.

Integrity. The property that data has not been altered or destroyed in an unauthorized manner. [ISO] The prevention of the unauthorized modification of information. [ITSEC] The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. [TCSEC]

Mechanism. An operating system entry point or separate operating system support program that performs a specific action or related group of actions.

Normal Operation. The process of using a system. [ITSEC]

Owner. A user who can modify the contents of an access control list.

Password. Confidential authentication information, usually composed of a string of characters. [ISO]

Privilege. A special authorization that is granted to particular users to perform security relevant operations.

Requirements. A phase of the Development Process wherein the top level definition of the functionality of the system is produced.

Resource. An operating system abstraction that is visible at the application program interface, has a unique name, and capable of being shared. In this document, the following are resources: files, programs, directories, databases, mini-disks, and special files. In this document, the following are not resources: records, blocks, pages, segments, bits, bytes, words, fields, and processors.

Security. The combination of confidentiality, integrity and availability. [ITSEC]

Security Relevant Event. Any event that attempts to change the security state of the system (e.g., change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (e.g., too many logon attempts). [TCSEC]

Security Audit Trail. Data collected and potentially used to facilitate a security audit. [ISO] A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. [TCSEC]

Shall. A requirement that must be met unless a justification of why it cannot be met is given and accepted.

Should. An objective that can be met. It is used when a specific requirement is not feasible in some situations or with common current technology. Non-conformance to such requirements requires less justification and should be more readily approved.

System. A specific IT installation, with a particular purpose and operational environment. [ITSEC]

User. The entity, human or machine, that is identified by the userID, authenticated prior to system access, the subject of all access control decisions, and held accountable via the audit reporting system.